One Step Forward, Two Steps Back?

University of Edinburgh
School of Law

Research Paper Series No 2013/17

Europa Working Series No 2013/7

One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework

Ms Judith Rauhofer
Lecturer in IT Law
University of Edinburgh, School of Law
judith.rauhofer@ed.ac.uk
To be published in the Journal of Law and Economic Regulation, Vol. 6, No. 1.

Abstract

Recent changes in market dynamics of electronic and mobile commerce mean that users of online services are no longer "passive agents of consumption". Instead online business models increasingly provide a platform for user interaction while simultaneously relying on the contributions made by those users for the population of those spaces. Like many other online services that form part of the Web 2.0 economy, SNS, in the main, are offered free at the point of access. Instead of charging their users a monetary fee, most SNS providers generate revenue through payments they receive from third parties in exchange for the right directly to display advertising to their users or in exchange for providing aggregated data on those users' behaviour, likes and dislikes. This means that users now "pay'" for online services with the personal information they disclose. Despite repeated announcements by members of the SNS industry that they are committed to the protection of their users' online privacy, it can therefore not be denied that, in practice, a high level of privacy protection is likely to be in stark conflict with SNS providers' business objectives and that, in reality, most SNS providers are entirely dependent for their market position on promoting an environment that encourages "openness" and widespread information-sharing by their users through the use of default privacy settings and the subtle encouragement of maximum disclosure in the form of financial and non-financial incentives (for example, additional "free" functionality). This article will examine the implications of these technical, economical and social developments of internet users' rights to privacy under the current EU data protection framework and whether the changes to that framework proposed by the European Commission in 2012 are likely to address the policy issues identified.

Keywords

privacy, data protection, consent, legitimate interest condition, social networking

One step forward, two steps back?

Critical observations on the proposed reform of the EU data protection framework

Judith Rauhofer[1]

Recent changes in market dynamics of electronic and mobile commerce mean that users of online services are no longer "passive agents of consumption". Instead online business models increasingly provide a platform for user interaction while simultaneously relying on the contributions made by those users for the population of those spaces. Nowhere is this more apparent than in the area of social networking where services like Facebook, LinkedIn, and Twitter allow customers to present an online version of themselves to others and to engage with friends, family and virtual strangers in online conversations.

A recent *Pew Internet survey*[2] found that in 2012, 67 per cent of all adult Internet users in the US used social networking services (SNS), up from 65 per cent in the previous year and 61 per cent in the year before. In the UK, the *Office of National Statistic's 2011 Statistical Bulletin on Internet Access* identifies social networking as one of the most popular online activities with 48 per cent of Internet users saying they took part in social networking[3]. SNS are increasingly embraced by older[4] as well as younger[5] users and their integration into everyday life is slowly changing the way in which individuals communicate, socialise, organise their lives, and engage with commercial players.

Despite the astounding increase in their user base over a relatively short period of time, one of the key challenges for SNS has always been the development of a credible monetisation strategy that encourages investment and allows for further innovation with a view to securing a foothold in a fast-changing market. Like many other online services that form part of the Web 2.0 economy, SNS, in the main, are offered free at the point of access. Instead of charging their users a monetary fee, most SNS providers generate revenue through payments they receive from third parties in exchange for the right directly to display advertising to their users or in exchange for providing aggregated data on those users' behaviour, likes and dislikes.

According to Gartner, worldwide social media revenue is expected to reach $16.9 billion in 2012, an increase of 43.1 per cent from 2011[6]. Of this amount $8.8 billion is said to derive from advertising revenue. New advertising models like social advertising and peer recommendations (for example, Facebook's "Like" and Google's "+1" buttons) only serve to illustrate further the online industry's continuing commitment to this business model and its resulting desire to maximise revenue through

---

[1] Lecturer in IT Law, University of Edinburgh.

[2] Pew Internet & American Life Project Poll, November 2012, available at http://www.pewinternet.org/Static-Pages/Data-Tools/Explore-Survey-Questions/Roper-Ce2ter.aspx?item={63EC8264-EF8F-4F38-B184-AB1D4B4E5FE4}, last visited on 23 April 2013.

[3] ONS Statistical Bulletin: Internet Access – Households and Individuals, 2012, 24 August 2012, available at http://www.ons.gov.uk/ons/dcp171778_275775.pdf, last visited on 23 April 2013.

[4] See Pew Internet: Social Networking 2012, available at http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx, last visited on 23 April 2013: the percentage of US internet users aged between 50-64 who use SNS rose from 47 percept in 2010 to 52 percept in 2012 while for those over 65 the increase was even steeper (from 26 percept in 2010 to 33 percept in 2011).

[5] The ONS 2011 Statistical Bulletin on Internet Access (see FN3) states that in the UK 91% of all 16-24 year old Internet users take part in social networking activities. According to the EU kids online survey carried out by the London School of Economics, 67% of children who use the Internet in the UK have their own social networking profile. This includes 28% of 9-10 year olds and 59% of 11- 12 year, despite the fact that most SNSs have a minimum age of 13 years; see L Haddon, and S Livingstone, "EU Kids Online: National perspectives", October 2012, p.69; available at http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/PerspectivesReport.pdf, last visited 26 October 2012.

[6] "Gartner Says Worldwide Social Media Revenue Forecast to Reach $16.9 Billion in 2012", 25 July 2012, available at https://www.gartner.com/it/page.jsp?id=2092217, last visited on 23 April 2013.

the tracking, monitoring and profiling of its user base according to their age, gender, interests, social class and financial acumen.

This means that users now "pay'" for online services with the personal information they disclose. Without that personal information, online platforms would lie empty and devoid of substance and SNS providers would not be able to produce the "product" (that is, the personal and behavioural data) from which they actually derive commercial value. Despite repeated announcements by members of the SNS industry that they are committed to the protection of their users' online privacy, it can therefore not be denied that, in practice, a high level of privacy protection is likely to be in stark conflict with SNS providers' business objectives and that, in reality, most SNS providers are entirely dependent for their market position on promoting an environment that encourages "openness" and widespread information-sharing by their users through the use of default privacy settings and the subtle encouragement of maximum disclosure in the form of financial and non-financial incentives (for example, additional "free" functionality).

Information privacy: a paradigm change?

One of the consequences of these developments in the online market place is the change that can be observed in the general attitude of individuals as well as public and private entities to the concept of information privacy as a whole. This concept is currently the subject of an intense struggle between those that argue in favour of preserving its traditional status as a fundamental human right and those who emphasise its utility as a quasi-property right that can be freely traded in an open marketplace.

Within most European countries, the right to a private life as protected by Article 8 of the European Convention on Human Rights (ECHR) and many national constitutions has, at least initially, largely been viewed in its public or constitutional law context as a defence against state interference. After the experiences during the Third Reich and WWII, an individual's ability to retire to a private sphere that is not observed and that allows him to process information and develop ideas and opinions without being subjected to undue influence was seen as an essential prerequisite for the active participation of the citizenry in political life and, thus, as a necessary safeguard of the democratic system itself.

As was first highlighted by Westin in 1969[7] and later confirmed by the German Constitutional Court in its *Census decision* in 1984[8], individuals must be able to exercise control over their own personal information. Where an individual is uncertain of who has access to their information in what context and for which purposes, he may feel inhibited in his actions, particularly if those actions challenge the dominant order or the policies of those in power. Someone who expects, for example, that his participation in a public protest or campaign will be officially registered and that this might expose him to negative reactions from employers or public bodies, will possibly refrain from participation in that protest despite the fact that his right to do so is itself protected as a fundamental right (freedom of assembly). According to Simitis, a loss of information privacy (or "informational self-determination") will therefore almost always also constitute a loss of "democratic substance"[9].

In a commercial context, the individual's right to control personal information about himself has initially largely been seen in the context of cases that concerned the misuse or misappropriation of personal information by others for their own commercial gain (for example, through faked celebrity endorsements or the exposure of the private life of public figures in the tabloid press). Claims against private parties based on Article 8 ECHR have been recognised by the European Court of Human Rights[10] and a system of sanctions and remedies in these cases has been developed in many European

---

[7] AF Westin (1967) "*Privacy and Freedom*", New York, Atheneum, p.7.
[8] "Census" decision, BverfGE 65, 1
[9] S Simitis (1984) "Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung", *Neue Juristische Wochenschrift*, pp.394-405 (399).
[10] See, for example, *Hannover v Germany* 40 EHRR 1, (2005).

countries. However, even in a private law setting the discussion within Europe commonly emphasises the issue of "control" identified above rather than the question of ownership of data[11].

The property-rights approach has always been promoted most successfully in the United States where the right to privacy, to the extent that it is recognised at all, is considered almost exclusively within the context of the private law domain. This was already apparent in Warren and Brandeis' famous 1890 article on "the right to be let alone"[12], which was said to be motivated by the authors' own experience of increasing press intrusion into their private affairs. Despite the fact that case law of the US Supreme Court also protects certain aspects of privacy as a defence against state intrusion under the Forth Amendment[13], the overwhelming majority of US "privacy" cases concern individuals' claims against other private entities.

US privacy law is thus composed almost entirely of a number of separate privacy torts identified and summarized by Prosser in 1960[14]. While a detailed examination of those torts is beyond the scope of this article, the restrictive way in which they are construed and the remedies and sanctions awarded emphasize both the proprietary and the commercial nature of the concept of privacy in this context. Privacy is thus seen as an instrument designed to ensure a kind of "parity of arms" between those who wish to use others' personal information for their own commercial benefit and those to whom that information relates and who should therefore be entitled to prevent such commercial exploitation or to derive some benefit or compensation in exchange.

Westin himself made this point that information privacy should be understood in the context of property rights when he argued that "personal information […] should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising"[15]. More recently, the model for "propertised personal information" has been revisited by several US scholars who have examined the arguments for and against a "market in personal information"[16] and who argue that a property-based approach to privacy is more likely to be successful in protecting individuals' personal information from unauthorized access by third parties. It is therefore possible to identify not just a legal but also a cultural and historical contrast between the EU and the US concept of privacy. It becomes increasingly clear that in order to arrive at a global solution to the new risks that the new online business models pose to their users' privacy, we will first have to address the different perceptions and consequent misunderstandings that dominate discussions between scholars and lawmakers on both sides of the Atlantic.

It is particularly interesting and illuminating to observe this on-going struggle for primacy in the area of privacy protection from the perspective of the UK that has itself strenuously resisted the introduction of a right to privacy in a domestic context for most of the 20th century. With an unwritten and flexible constitution, the UK lacks a traditional understanding of privacy as a fundamental right. Although the UK is a signatory of the ECHR and is therefore required to comply with its Article 8, no **national** catalogue of basic rights includes a specific right to privacy. Similarly, in the private law domain no "privacy laws" were ever adopted by the UK Parliament. As recently as 1991, the English Court of Appeal was able to maintain that no tort of privacy existed in English law[17], which left citizens largely unprotected against intrusions, in particular, by the tabloid press.

---

[11] J.E.J. (Corien) Prins (2006) "Property and Privacy: European Perspectives and the Commodification of Our Identity", *Information Law Series*, Vol. 16, pp. 223-257 (257).

[12] S Warren and LB Brandeis (1890) "The right to privacy", Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

[13] Going back to its decision in *Katz v United States* 389 U.S. 347 in 1967, where it limited the right of law enforcement authorities to intercept citizens' telephone conversations.

[14] D Prosser (1960) "Privacy", 48 *California Law Review* 383.

[15] Ibid. at FN7.

[16] See, for example, KC Laudon (1996) "Markets and Privacy", 39 *Communications of the ACM* 92-104; J Litmann (2000) "Information Privacy/Information Property", 52 *Stanford Law Review* 1283-1313; PM Schwartz, (2004) "Property, Privacy, and Personal Data", *Harvard Law Review*, Vol. 117, Vol. 7, p. 2055. For the European perspective, see J.E.J. (Corien) Prins (2006) "Property and Privacy: European Perspectives and the Commodification of Our Identity", *Information Law Series*, Vol. 16, pp. 223-257.

[17] *Kaye v Robertson* [1991] FSR 62.

This situation only changed fairly recently as a result of two important changes to the UK legal framework. First, by virtue of its membership of the European Community (now the European Union), the UK was required to transpose the EC Data Protection Directive[18] into national law through the adoption of the Data Protection Act 1998 (DPA). Around the same time, the then Labour government decided to adopt the Human Rights Act 1998 (HRA) which came into force in 2000. While the DPA created a solid legal framework for the processing of personal data by public and private bodies, the HRA enabled UK citizens for the first time to enforce the rights guaranteed by the ECHR in the domestic courts.

These events, which represent a principal point of departure in the development of privacy law in the UK, sparked a number of court cases – mainly instigated by celebrities and well-known public figures - which permitted the courts to carve out a rudimentary right to privacy. This right is currently based both, on the provisions of the DPA as well as a reinterpretation of the tort of breach of confidence. Mirroring the developments in the US, this tort now prohibits the "wrongful" or "unjustified disclosure of private information"[19]. However, its provenance is shady to say the least, marrying, as it does, a European fundamental rights approach with a US-style property rights approach without ever fully embracing or dismissing either.

Information privacy in the context of the EU data protection framework

Despite the attention the UK courts received when they developed the new right to privacy in its private law context, on a day-to-day basis, the requirements of the DPA are likely to have had by far the greater impact on UK and non-UK businesses. When examining the history of data protection law in Europe, it can immediately be established that it owes much of its existence not only to a general desire to protect the individual from arbitrary or unaccountable decision-making by public and private bodies, but also to a contrasting desire to facilitate the processing of personal information for public policy as well as commercial objectives.

On the one hand, the modern information technology systems, which came into widespread use during the 60s, 70s and 80s and which enabled the automated processing, combining, searching and sharing of information, alerted lawmakers in many countries to the need for measures that would prevent the misuse of that information. On the other hand, the new technology also opened up new ways of achieving administrative, economical and commercial benefits by making the use of personal information more efficient and by facilitating new administrative and commercial uses of that information. New work processes and business models were being developed that required the transfer of personal information between different parties and across national borders. In this context, the spectre of overly strict data protection laws led to concerns that their adoption might either lead to the development of "data havens" elsewhere (and might thus create a competitive disadvantage for the businesses established in the countries that adopted those laws) or might restrict transborder data flows to countries without adequate protection. Data protection laws were therefore often seen by others - including in particular the United States with its dominance in the information and information technology industry – as "unduly restrictive and blatantly protectionist"[20].

As a result, the data protection laws that did eventually develop, both at national and international level, in almost all cases sought to strike a balance between, on the one hand, the individual's and

---

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23.11.1995. Although the UK had previously adopted its own Data Protection Act 1984, the protection afforded by this Act fell significantly below the level which existed in other EU member states at the time.

[19] See, for example, *Campbell v MGN Ltd* [2004] UKHL 22; *Douglas and others v Hello! Ltd and others* [2005] EWCA Civ 595; *McKennitt and others v Ash and another* [2005] EWHC 3003; *CC v AB* [2006] EWHC 3083; *Murray v Express Newspapers plc and another* [2007] EWHC 1908 (Ch); *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB); and *John Terry (previously referred to as "LNS") v Persons Unknown* [2010] EWHC 119 (QB

[20] J Moakes 'Data protection in Europe – Part 1' (1986) 1 *Journal of International Banking Law* 77 (82)

society's need for the protection of personal information and, on the other hand, the need of businesses and public bodies for the free flow of data.

This is true for most of the early international instruments, including the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[21] and the *Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[22], but also for the more detailed EU data protection framework that was developed a decade later. That framework includes, among other things, the 1995 Data Protection Directive[23], the 2001 EC Data Protection Regulation governing processing activities by the EU institutions[24], and the 2002 E-Privacy Directive[25] (as amended by the 2009 Consumer Rights Directive[26]). Going forward, the twin objectives have also been recognised more recently at EU constitutional level in the form of Article 16 of the Treaty on the Functioning of the European Union (TFEU)[27] and Article 8 of the EU Charter of Fundamental Human Rights[28] ("Protection of personal data"), which came into force in December 2009.

The common denominator between all of these instruments - and the way in which they put those twin objectives into practice - is that they are framed in terms of a number of "fair processing principles" to be observed by those wishing to process personal data. Those principles are founded on the basic assumption that any processing of personal data must either be authorised by the data subject giving his consent or must be limited to that which is necessary for certain commercial or public policy purposes. While there are certain analogies between the "consent" condition and the property-rights approach described above, the other policy-based conditions that form part of the fair processing paradigm provide additional legal grounds for processing. The fair processing paradigm has therefore been criticised for providing a lower level of protection to individuals compared to the property-rights approach precisely because the latter, at first glance, seems to prohibit **all** processing that is not specifically authorised by the "owner" of the data, while the fair processing paradigm makes room for additional justifications.

However, this argument ignores the fact that within any society personal data processing without an individual's consent may at times be reasonably necessary in the public interest, in the interest of other parties and even in the individual's own interest (for example, where he is prevented from giving his consent in case of illness or accident). It is therefore likely that even jurisdictions that generally follow a property-rights approach would legislate for certain exceptions in these situations (national security, public health and crime prevention easily spring to mind in this context). The question to be answered in those cases is therefore not whether any exceptions to the individual's right to control access to their personal data should be provided for at all, but whether a fundamental rights framework exists in a given jurisdiction which limits the legislator's right to erode the general right to privacy through an abundance of permissive legal provisions.

---

[21] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980, available at http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, last visied at 27 October 2012

[22] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted on 28 January 1981, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, last visited on 27 October 2012

[23] See FN18.

[24] Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.1.2001

[25] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 , 31.07.2002.

[26] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009.

[27] OJ C 83/47, 30.3.2010. Article 16 provides that "everyone has the right to the protection of personal data concerning them", but also makes it clear that any EU legislation in this area must address "the rules relating to the free movement of such data".

[28] OJ C83/389, 30.3.2010. The official JUSTICE commentary on Article 8 emphasises that the EU data protection framework, including the Charter, was developed "[i]n order to promote th[e] free exchange of information *while also respecting* the privacy rights of individuals"(emphasis by the author); see JUSTICE commentary on Article 8 of the EU Charter of Fundamental Rights; available at http://www.eucharter.org/home.php?page_id=82, last visited on 29 October 2012.

More importantly, though, both the property-rights and the consent approach to privacy rests on the fundamental assumption that individuals will act rationally and in their own best interest when making decisions about the disclosure to, or use by, others of their personal data. In light of recent developments particularly in the online arena, this assumption may have to be revisited. To begin with, the by now well-established "privacy paradox"[29], that is, the tendency of individuals, on the one hand to state that they value privacy while simultaneously engaging in behavior that puts that privacy at risk (for example, the disclosure of information on SNS or the use of loyalty cards) shows that most individuals do not join the "open marketplace" for their personal information as quite the rational actors that much economical theory presumes them to be[30].

Furthermore, data subjects are often at risk of inadvertently losing control over their personal information when dealing with those on whom they depend for the provision of jobs, information, goods or services. In almost all cases, dependency creates an intrinsic power imbalance, which is likely to enable the stronger party to put pressure on the weaker one or to manipulate it in often subtle and hence potentially unaccountable ways. In the context of data protection, this may mean that the stronger party might use its power over the weaker party to effectively force it to consent to certain processing activities.

This phenomenon is well understood with regard to the more traditional relationships, for example, employer/employee relationships, where many data protection regulators have already interpreted the fact that consent must be "freely given" to mean that, in practice, this all but excludes employers' ability to process employee data solely on the basis of the employee's consent[31]. It could increasingly be argued, that a comparable power imbalance may determine much of the relationship between Internet users and online service providers, particularly in areas where a lack of competition restricts the user's choice of provider.

The question therefore is not only whether the property-based approach or the fair processing/fundamental rights approach is more suitable to ensure the protection of individuals' personal information, but which additional regulatory safeguards might be necessary with regard to both approaches.

Data protection compliance in an SNS context

Viewing the US and the EU systems side by side, the regulatory burden imposed on US-based companies is significantly lower than that of their EU counterparts. While some requirements exist with regard to information security and data security breaches[32], US SNS providers are by and large free to process as much of their users' personal information as those users are willing to disclose to them[33]. In this situation, it is easy to the see the attraction of a property-rights approach, as this would ensure some protection for those users willing and able to negotiate access to their personal data.

---

[29] See, for example, PA. Norberg, DR Horne, DA Horne (2007) "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *Journal of Consumer Affairs*, Volume 41, Issue 1, pp. 100–126; NF Awad and MS Krishnan (2006) "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization", *MIS Quarterly*, Vol. 30, No. 1, pp. 13-28; V Groom and MR Calo (2011) "Reversing the Privacy Paradox: An Experimental Study", TPRC 2011. Available at SSRN: http://ssrn.com/abstract=1993125.

[30] For recent economical theory on privacy and rational behavior, see also A Acquisti and J Grossklag (2005) "Privacy and Rationality in Individual Decision Making", *EEE Security & Privacy*, January/February 2005, pp. 24-30; available at http://csis.pace.edu/~ctappert/dps/d861-09/team2-3.pdf, last visited on 29 October 2012.

[31] See for example, paragraph 24, section B9 of the UK Information Commissioner's "*Guide to Data Protection*", which states that consent should not be relied upon where the data subject has no real choice but to give it; available at http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx, last visited on 29 October 2012.

[32] See, for example, California's Notice of Security Breach law (Cal. Civil Code §1798.29).

[33] Companies providing sub-contracted data processing services to EU data controllers may be caught by the EU regulatory framework through the application of the adequacy principles included in Article 25(1) of the Data Protection Directive (implemented in the UK through the eighth data protection principle, paragraph 8, Part I, Schedule 1, DPA). This restricts the transfer of personal data to countries outside the European Economic Area to those countries that have in place adequate protection of personal data or where adequacy can be otherwise adduced. A transfer to a US company is generally permitted provided that company has signed up to the safe harbour framework enforced, in the main, by the US Federal Trade Commission (see http://export.gov/safeharbor/). In addition, data processing activities of US SNS providers may fall within the territorial scope of the EU data protection regime, if one of the conditions set out in Article 4(1) of the Data Protection is fulfilled. This includes cases

SNS providers that are established in an EU member state, on the other hand, fall within the scope of the EU data protection framework (as implemented by the relevant member state). SNS providers commonly aim to achieve compliance with the requirements of that framework through a mixture of contractual agreements (including terms of business and privacy policies), technical features (including privacy settings and defaults) and industry standards and self-regulation. In a 2009 opinion on how the operation of SNS can meet the requirements of EU data protection legislation[34], the EU's Article 29 Working Party made it clear that both SNS providers and providers of individual applications on SNS are data controllers under Article 2(d) of the Data Protection Directive[35]. This means that SNS providers must comply with the provisions of national legislation implementing that Directive and the E-Privacy Directive when collecting and further processing their users' personal data.

To ensure compliance, SNS providers must, among other things, provide their users with certain fair processing information about the provider's identity and the purposes for which they intend to process users' personal data. This fair processing information must be provided before the start of the data processing activities[36], that is, before or at the point of collection. In practice, providers will often include this information in their terms of business and their privacy policies. Nevertheless, the fair information requirement has been criticised by many data controllers as unduly burdensome, particularly in areas, where the risk of material harm is low.

In addition to the fair processing requirement, Article 7(1) of the Data Protection Directive (implemented in the UK through Schedule 2 of the DPA) provides that personal data may only be processed if one of a number of enumerative conditions is met[37]. In addition to the data subject's consent, processing is lawful if it is necessary to perform a contract with the individual, to comply with a legal obligation of the provider (for example, in order to establish the age of the user) or for the legitimate interests of the provider or a third party to whom the provider discloses the data (except where it is unwarranted because it is prejudicial to the individual).

The data protection framework only applies to the processing of "personal data". As the use of electronic communications systems and online services generates several new types of data, which lawmakers did not specifically take into account when the Data Protection Directive was adopted in 1995, there has been some discussion recently about whether its material scope is still appropriate for the digital age.

In the majority of cases, SNS providers and providers of applications offered to SNS users rely on users' consent. In the UK, this consent is usually obtained by implying users' acceptance of a privacy policy either through specific consent wording in the policy itself or through a statement on the sign-up page, which the user must acknowledge by ticking a box or clicking a button[38].

Of the other available legal grounds on which data controllers may rely to justify their processing activities in the absence of user consent, the condition contained in Article 7(f) of the Data Protection Directive ("processing for the legitimate interest of the data controller or a third party") can probably be seen as facilitating the most permissive processing of personal data.

However, in response to complaints from both industry and civil society that the Directive is increasingly out of date, The EU institutions are currently discussing a reform of the EU data protection

---

where the processing is carried out in the context of the activities of a branch office that the US company has established in an EU member state or if the processor makes use of equipment situated in a member state as part of their processing activities.

[34] Article 29 Working Party, Opinion 5/2009 on online social networking, 12 June 2009.

[35] In the UK, this definition is mirrored in section 1(1), DPA.

[36] In the UK, this requirement is included in the first data protection principle, paragraph 1, Part I and paragraphs 1-4, Part II to Schedule 1, DPA.

[37] For a detailed interpretation of the "enumerative" nature of the legal grounds contained in Article 7(1), see the ECJ's decision in *Asociación Nacional de Establecimientos Financieros de Crédito and Federación de Comercio Electrónico y Marketing Directo v Administración del Estado* Joined cases C-468/10 and C-469/10, 24 November 2011.

[38] See below for a more detailed description of the UK's approach to obtaining consent.

framework, which is specifically intended to adapt that framework to the new technological reality[39]. The relevant changes proposed in this respect will be the focus of the remainder of this article.

EU data protection reform

In January 2012, the European Commission published its long-awaited proposals for the revision of the Data Protection Directive[40]. The centrepiece of the reform package is a draft Regulation[41] that would replace the existing regime. The reform proposals follow several years of discussions at EU and member state level, including two stakeholder consultations (in 2009[42] and 2010[43]) and the publication by the European Commission of a Communication "*A comprehensive approach on personal data protection in the European Union*"[44] in November 2010.

The draft Regulation contains measures that would harmonise data protection procedures and enforcement across the EU, and achieve consistency with the existing system for ensuring privacy online set out in the E-Privacy Directive. It would also expand the application of the EU regime to data controllers that are not established in the EU but whose processing activities are related to (1) the offering of goods or services to EU data subjects; or (2) the monitoring of those data subjects' behaviour[45]. This would bring the majority of SNS providers within the reach of the new regime, even if they do not operate a branch office in an EU member state. The governments of many non-EU countries and particularly the US, where nearly all of the most popular SNS providers are established, therefore closely watch the progress of the reform proposals.

The draft Regulation includes nine substantive chapters, covering among other things the subject matter and scope of the Regulation, revised definitions, revised data protection principles, new obligations on data controllers and data processors and a revised framework for the transfer of personal data to third countries or international institutions. The Regulation would be directly binding on data controllers immediately upon coming into force without the need for implementation by the member states[46].

The explanatory memorandum accompanying the draft Regulation specifically acknowledges the impact that technological change has had on the existing framework and the need for reform. Recital 5 of the draft Regulation also highlights the fact that:

> *"[r]apid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally[47]".*

---

[39] See the Explanatory memorandum accompanying the draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.1.2012, COM(2012) 11 final, p. 1.

[40] Commission press release "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", 25 January 2012, available at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, last visited on 30 October 2012; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century", COM/2012/09 final.

[41] See FN39.

[42] "Consultation on the legal framework for the fundamental right to protection of personal data", 31.12.2009, available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm, last visited on 30 October 2012.

[43] "Consultation on the Commission's comprehensive approach on personal data protection in the European Union", 4. 11.2012, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm, last visited on 30 October 2012.

[44] COM(2010) 609 final, 4.11.2010.

[45] Article 3(2), draft Data Protection Regulation.

[46] Article 288, TFEU.

[47] Recital 5, Draft General Data Protection Regulation,

The Recital specifically emphasises the economical impact that technological development has had and the explanatory memorandum highlights the information economy's central role in the Digital Agenda for Europe[48], and more generally in the Europe 2020 Strategy[49]. It sees the reform as an opportunity to further facilitate the free flow of data within the European Union and the transfer to third countries and international organisations with a view to encouraging new means of communication, new business models and economic growth.

The explanatory memorandum professes that this can be done while still ensuring a high level of privacy protection within the EU. However, there has been no shortage of criticism from privacy advocates[50], who claim that the draft Regulation is in danger of upsetting the delicate balance between the two objectives that have defined the EU data protection framework for the past decades and that any additional safeguards it offers to protect individuals' privacy rights in the online environment are offset by other provisions that grant data controllers more extensive rights to collect and process personal data. Of the many fault lines identified by those privacy advocates in this context, this article will look more closely at only two that affect the processing operations of SNS, namely the changes proposed to the legitimate interest condition and the concept of consent.

Legitimate interest

Under Article 7(1) of the Data Protection Directive (implemented in the UK through paragraph 6 of Schedule 2 to the DPA), SNS providers may be able to justify their processing activities on the grounds that such processing is necessary for the purpose of their legitimate interest or the legitimate interest of third parties to whom they disclose their users' personal data. This legal ground is subject to an exception where "the interests or fundamental rights and freedoms of the data subject" override such interests.

In practice, this means, that data controllers can undertake a wide range of processing activities without the data subject's consent, provided that these activities are in some way related, among other things, to their commercial aims and objectives. Both in the UK and at EU level, very little guidance is available on how the legitimate interest condition is to be interpreted. The ICO, in legal guidance which has since been replace by its - in this context at least, less informative "Guide to Data Protection" - indicated that it intended to "take a wide view of the legitimate interests condition" [51]. It suggested that it would apply two tests to establish whether this condition may be appropriate in any particular case. First it would dermine the legitimacy of the interests pursued by the data controller or the third party to whom the data are to be disclosed, and second, it would establish whether the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject that override those of the data controller. The ICO's legal guidance specifically highlighted that "[t]he fact that the processing of the personal data may prejudice a particular data subject does not necessarily render the whole processing operation prejudicial to all the data subjects"[52].

---

[48] COM(2010)245 final.

[49] COM(2010)2020 final.

[50] See for example, D Korff (2012) "Comments on Selected Topics in the Draft EU Data Protection Regulation - Summaries and Proposed Amendments Only", available at SSRN: http://ssrn.com/abstract=2150151 or http://dx.doi.org/10.2139/ssrn.2150151; European Digital Rights: Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at http://edri.org/files/1012EDRi_full_position.pdf; Article 29 Working Party Opinion 01/2012 on the data protection reform proposals (WP191), 23 March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf; Article 29 Working Party Opinion 08/2012 providing further input on the data protection reform discussions (WP199), 5 October 2012, ttp://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf; and EDPS Opinion on the data protection reform package, 7 March 2012, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, all last visited on 31 October 2012.

[51] ICO "Data Protection Act 1998 - Legal Guidance", pp. 20-21, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf, last visited 1 November 2012.

[52] ibid.

Applying these two tests, one could imagine, for example, that the following activities might fall within the scope of the legitimate interest condition: a data controller's interest in marketing its goods or services, including the data mining and profiling that, in the online environment is often a prerequisite for such marketing; an employer's interest in monitoring its employees' performance, and even a company's interest in selling its customer database as part of its assets. The problem in many cases is likely to be that, at least in the short term, none of these activities seem to cause any actual harm to, or seem to affect the interests of, the data subject. However, the question that has not yet been sufficiently explored is what long-term effect these activities may have not only on individual data subjects, but also on the distribution of powers between certain categories of data controllers and data subjects. If, for instance, online providers can use this condition to establish a large database about their users' personal circumstance, likes and dislikes, to what extent does this affect their bargaining position vis-a-vis those users in the future? The old adage that "information is power" springs to mind in this context, and it is difficult to deny that, if two parties have at their disposal very different amounts of information about each other when considering the conditions on which they are prepared to enter into a contractual relationship, the odds - during the contractual bargaining - are likely to be stacked in favour of the party that knows more about the other party. In addition, there are other potential long-term consequences that could arise for the interests of data subjects through the mere fact that their data is stored by a data controller, for example, information and data security issues. There is also the possibility that the data might be made available, voluntarily or because of a legal obligation, to third parties without the data subject's consent in the future, thereby possibly establishing an entirely new set of power imbalances that affect the data subject's rights.

The wide interpretation of the legitimate interest condition combined with a seemingly omnipresent desire to collect ever more personal data "just in case" for the purposes of risk management[53] therefore severely affects the principle of control that defines the concept of information privacy and that is otherwise intended to underpin the existing data protection framework. Without more specific guidance on which of the data controller's interests can be viewed as "legitimate" it could be said that this condition is able to drive a horse and carriage through the protection afforded to data subjects by the existing data protection regime.

Going forward, the existing condition is mirrored to a large extent in Article 6(1)(f) of the draft Regulation. However, Article 19 of the draft Regulation now grants the data subject a "right to object" to processing that is being conducted without his consent. While much of this right is based on Article 14 of the existing Directive, it includes some significant modifications regarding the burden of proof and its application to direct marketing. Where this right is exercised, the processing must stop.

Under Article 14 of the Data Protection Directive, the burden of proof for establishing that his interests or rights and freedoms override the legitimate interests of the data controller falls on the data subject. This means that the data subject has to prove that compelling legal grounds exist for why the processing should **not** take place. If the data subject is unable to provide evidence for this contention, the controller's processing activities are deemed to be lawful.

In contrast, Article 19(1) of the draft Regulation grants the data subject a right to object, on grounds related to his personal situation, to **any** processing justified by the data controller on the basis of, among other things, Article 6(1)(f). This means that the data subject's right to prevent such processing exists *ab initio,* and it now falls to the data controller to demonstrate that he has compelling legitimate grounds for the processing which override the data subject's interests or fundamental rights and freedoms.

---

[53] For a detailed examination of the relationship between risk awareness and the willingness to disclose personal information, see J Rauhofer (2008) "'Privacy is dead, get over it!' Information privacy and the dream of a risk-free society", Information and Communications Technology Law Vol. 17 Issue 3, pp. 185-197

This effectively constitutes a reversal of the burden of proof compared to the current situation, which will make it more difficult for the data controller to rely on legitimate interest grounds to justify his processing activates. In practice, this will particularly affect data controllers who habitually rely on the "legitimate interest" condition. If the provision is adopted in this form, data controllers may therefore, at first glance, find it considerably more difficult to justify certain processing activities under the new regime. Both the concepts of "necessity" and "compelling legitimate grounds" now seem to be weighed heavily in favour of the data subject.

However, the practical effect of this reversal of the burden of proof may be significantly lessened by the complexity of the provision, the intricacies of which may escape many an average data subject. Although, Recital 38 and Article 14(1)(b) promote more transparency by imposing an obligation on the data controller to explicitly inform the data subject about the legitimate interests pursued and on the data subject's right to object, judging on past form, few data subjects, particularly in the online environment, will take much notice of the ever increasing amount of "fair processing information" directed at them and will thus often not be aware of their right to object. Even where such awareness can be created through the additional obligation set out in Recital 38, many data subjects will still feel that they do not have the bargaining power to resist the collection and further processing of their data. Similarly, the fact that Article 28(2)(c) obliges the data controller to document his legitimate interests as part of his wider documentation obligations is unlikely to have much practical impact on the decision-making powers of the average data subject. The mere fact that data subjects must invoke their overriding interests and that, unless data subjects exercise their right to object, the proposed processing activity is deemed to be lawful, sits uneasily with experiences of current levels of user inertia. Although some would argue that data subjects should be expected to accept a certain amount of personal responsibility for protecting their own information, it is more than likely that on current levels of awareness, skill and education, the majority of data subjects will just not benefit from the revisions of the legal framework currently under consideration.

What the Regulation, like its predecessor, specifically lacks at this stage is sufficient guidance on which of the data controller's interests can be considered "legitimate". Some attempts to provide such guidance can be found in Recital 39, which makes it clear that data processing for the purposes of ensuring network and information security constitutes a legitimate interest of the concerned data controller. But save for this provision, any determination of this question is postponed to a later stage through Article 6(5) of the draft Regulation, which grants powers to the European Commission to adopt delegated acts for this purpose. This approach can be criticized for several reasons.

First, Article 6(5) leaves the right to make vital decisions about the practical implementation of one of the most popular legal grounds for data processing to an executive body, which has limited legitimacy for making those determinations. As some observers, including, for example, the EDPS, have already highlighted, the extensive use of delegated powers in the draft Regulation may in fact violate Article 290(1) TFEU[54], which restricts the use of delegated acts to non-essential elements. It could be argued that the concrete form of the legitimate interest condition should be considered an essential element to be included in the draft Regulation itself, given the condition's practical impact, both qualitatively and quantitatively, on the rights of the data subject.

Second, even if one were to accept that the further clarification of the condition can be deferred to a point after the adoption of the Regulation, the European Commission seems a curious choice as the body tasked with the interpretation of data protection laws when, until now, guidance on the meaning of specific legal provisions has been provided by the Article 29 Working Party and the national data protection authorities. The Commission, in its role as a policymaker, is arguable more susceptible to well-funded lobbying from industry stakeholders than most independent regulatory bodies would be. There is therefore a danger that the process of determining what the appropriate balance between the interests of data subjects and data controllers should be in this context would suffer from reduced scrutiny and accountability. A more intuitive approach would therefore be to grant these powers to the

[54] FN50, paragraph 74.

body replacing the Working Party at EU level and representing the opinions of the national authorities, namely the new European Data Protection Board (EDPB) to be set up under Article 64(1) of the draft Regulation.

Finally, the possible time lag between the coming into force of the Regulation and the time at which the Commission may be ready to adopt the relevant delegated act may leave a regulatory vacuum which could easily be filled by developing market practice that itself might then influence the Commission's judgment on which interests should be considered legitimate.

From a policy point of view, the question therefore arises whether more wide-ranging protections are not necessary to achieve the intended aim of Article 19 of the draft Regulation better to protect the data subject's position vis a vis the data controller with regard to the legitimate interest condition.

The European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), which at the time of writing scrutinizes the draft Regulation as part of the legislative process, has picked up many of these points in the draft report it published in January 2013[55]. It suggests that the legitimate interest condition should only provide a legal basis for processing in "exceptional circumstance"[56] and dismisses the idea that the power to further clarify the legitimate interest condition should lie with the Commission. Instead, it recommends that Article 6(5) should be deleted and that Article 6(1)(f) should be replaced with much more detailed guidance designed to provide legal certainty to the data controller. To achieve this aim the draft LIBE report proposes to insert new provisions into the draft Regulation, which deal respectively with issues of transparency, the question of what should constitute the data controller's legitimate interest and the question of how the data subject's overriding interests should be defined.

New Article 6(1a) includes a binding requirement on the data controller specifically to inform the data subject if it processes the data subject's personal data for the purposes of his legitimate interest[57]. The notification must also set out the data controller's reasons for believing that its interests override the interests or fundamental rights and freedoms of the data subject. Article 6(1b) lists the specific circumstances in which the data controller's interests may override the interests of the data subject. They include the data controller's freedom of expression, processing for the enforcement of legal claims or for preventing or limiting damage to the controller, further processing for direct marketing of the controller's own goods or services, processing in the context of professional business-to-business relationships and processing by not-for-profit organisations for the sole purpose of collecting donations. In addition, Recital 39 clarifies that network and information security constitute a legitimate interest. Article 6(1c) lists the specific circumstances in which the data subject's interests override the legitimate interest of the data controller. This is particularly the case when the processing causes a serious risk of damage to the data subject, when sensitive personal data, location data or biometric data is processed, when the data is processed in the context of profiling or when it is made accessible to a large number of people or where large amounts of data is processed or combined with other data, where processing may lead to discrimination against the data subject, and where the data subject is a child.

Although the LIBE proposals would go some way towards addressing the issues regarding the legitimate interest condition, there is some doubt over whether or not they will survive even the negotiations between the different parliamentary committees involved in the scrutiny of the draft Regulation. At the time of writing, the LIBE Committee has received over 3000 amendments, some of which are included in opinions submitted by other committees, some were submitted by individual members of the European Parliament. A group of individual privacy organisations that has examined those

---

[55] Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD), 16.01.2013. Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN; last visited on 12 January 2013.

[56] ibid., proposed amendment to Recital 38.

[57] In the Commission's January 2012 draft, such a requirement is only included in Recital 38.

amendments has published a report in April 2013[58], in which it highlights that rather than "fixing" the issues raised in respect of Article 6(1)(f), MEPs are seeking to maintain the existencing broad condition[59] or even to extend its use by proposing that the data controller's"rights and freedoms to conduct a business" should be balanced against the rights and freedoms of the data subject[60]. The LIBE Committee is currently expected to adopt its final report in the summer 2013. This would then provide the basis for the European Parliament's negotians with the European Council.

There is a clear argument that a clarification of the legitimate interest condition could provide legal certainty and thus save data controllers costs. A tighter regulatory framework might also generate increased trust on the part of data subjects that they will not loose control over their personal information if they disclose that information when using online services. This, in turn, could lead to an increased uptake of those services, which would benefit the digital economy as a whole.

Consent

There is currently some uncertainty about the exact nature of consent in a data protection context. Article 2(h) of the Data Protection Directive defines consent as the "freely given, specific and informed" indication of the data subject's wishes by which he signifies his agreement to personal data relating to him being processed. However, EU member states differ in their implementation of this provision[61] and in recent months, a chasm has arisen on the interpretation of the limits of consent between the Article 29 Working Party and the EDPS on the one hand and the ICO on the other.

The DPA does not specifically define consent, although national courts need to interpret this term by reference to the Data Protection Directive. However, while other EU regulators as well as the EDPS and the Article 29 Working Party have repeatedly advocated a restrictive interpretation - rejecting, for example, the practice of using pre-ticked boxes to imply consent and arguing in favour of a restriction on consent in situation where there is an unequal relationship between the data subject and the data controller[62] – the ICO has always taken a more relaxed attitude to the concept and, particularly, the way in which consent can be obtained.

The conflict between the institutions came to a head with regard to the interpretation of the consent requirement for the setting of cookies that was inserted into Article 5(3) of the E-Privacy Directive by the Citizens' Rights Directive in 2009. After initially following the Working Party's fairly restrictive guidance on the interpretation of consent, the ICO decided to depart from that position in its most recent guidance on the use of cookies[63], published in May 2012, where it specifically permitted the use of "implied" consent contrary to the Working Party's own guidance.

---

[58] International privacy organisations "Don't let corporations strip citizens of their right to privacy"; available at http://edri.org/files/2013-campaign-report.pdf; last visited on 25 March 2013.

[59] AM880 (Louis Michel, ALDE), AM882 (Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, EPP), AM883 (Salvatore Iacolino, EPP) and AM884 (Ewald Stadler) to the draft report by Jan Philip Albrecht, 4 March 2013; available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-506.145%2b01%2bDOC%2bPDF%2bV0%2f%2fEN; and AM47, Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 March 2013; available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-494.710%2b02%2bDOC%2bPDF%2bV0%2f%2fEN; AM100, Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairson the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 26 February 2013; available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-496.562%2b02%2bDOC%2bPDF%2bV0%2f%2fEN; last visitied on 25 April 2013.

[60] ibid., AM873 (Alexander Alvaro, Nadja Hirsch, ALDE), AM874 (Adina-Ioana Vălean, Jens Rohde, ALDE)

[61] For an overview of the concept of consent in EU data protection law, see E Kosta (2013) "*Consent in European Data Protection Law*", Brill Academic Publishers, Inc.

[62] See, for example, Article 29 Working Party, Working Document on a common interpretation of Article 26(1), adopted on 25 November 2005, WP114; Article 29 Working Party Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171; and Article 29 Working Party Opinion 15/2011 on the definition of consent, 13 July 2011, WP187.

[63] ICO: Guidance on the rules on use of cookies and similar technologies, v.3, May 2012.

The predominant issue with the use of consent in a data protection context lies in the fact that the privacy policies which online providers commonly use to imply their users' consent to the processing of their personal data in many cases lack transparency and that providers have taken advantage of the loose regulatory framework which imposes no restrictions on the purposes to which users may consent. Until recently, it was therefore widely felt that a well-written privacy policy can easily be employed to obtain *carte blanche* for almost any processing purpose providers can envisage now or in the future, and it is perhaps unsurprising that the length of privacy policies has increased dramatically in recent years as providers have added more and more purposes to their lists.

To illustrate this point, the New York Times published a graphic created by private user Matt McKeon in 2010, which shows that the privacy policy used by SNS Facebook had ballooned from 1004 words in 2005 to 5,830 words in 2010[64]. Its current data use policy[65] is layered and consists of six main sections and, although designed to be more user friendly, is significantly longer. This volume of legalese and the often confusing way in which the information is arranged gives new meaning to the phrase 'hidden in the small print' and is likely to challenge even the most dedicated user. A lack of skill combined with the feeling that nothing can be done to change those policies in any case causes the majority of users to simply agree to them without ever reading them. This has made it easy for providers to argue that their users have in fact sanctioned all of the provider's data processing activities. However, in light of the clear failings of this approach we must ask ourselves whether, in an environment where this type of behaviour is technically possible and legally permitted, user consent is still an adequate tool for the authorisation of what constitutes an increasingly severe intrusion into users' private life.

Interestingly, the issue of privacy policies that are too general and cover too wide an array of data types and purposes was recently taken up by the Article 29 Working Party with regard to the Google privacy policy. In March 2012, Google updated its terms of service and consolidated over 60 of its privacy policies into one single privacy policy with a view to aggregating its users' personal data from across all their accounts and services including: Gmail, Google Play, Google+, internet searching, map, YouTube, location data and photo sharing. This prompted the Working Party to ask the French data protection regulator, CNiL, to lead an investigation into Google's new policy on behalf of the national data protection authorities of all member states, and to examine whether Google complies with the requirements set out in the Data Protection Directive. In October 2012, the EU data protection authorities published their findings[66]. Among other things, the authorities found that Google may have failed to comply with the Data Protection Directive on a number of counts, namely the information requirements; the fair and lawful processing requirements; the requirements guaranteeing the data subject's right to object to the processing of their personal data; and the right to request erasure or blocking of that data. Considering, in particular, the legal grounds for processing personal data on the basis of (1) user consent, and (2) legitimate business interest and contract performance, the findings could not establish a valid legal ground for the processing in the case of four of the eight purposes named in the policy. In particular, the CNiL's findings reiterate that Google cannot rely on user consent in cases where the user is not aware of the exact extent of the combination of the data between different Google services[67].

---

[64] 'Facebook Privacy: A Bewildering Tangle of Options', New York Times online edition at http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html (last visited 19 May 2010).

[65] Facebook data use policy; available at http://www.facebook.com/about/privacy/; last visited on 25 April 2013.

[66] Google Privacy Policy: Main Findings and Recommendation, 16 October 2012, available at http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf, last visited on 30 October 2012.

[67] As Google had not implemented any of the significant compliance measures suggested by the CNiL by April 2013, the data protection authorities of France, Germany, Italy, the Netherlands, Spain and the UK have announced that they will take consolidated action against Google to examine whether its privacy policy complies with their respective national data protection legislation. To this end, they have initiated an inspection procedure and set up an international administrative co-operation procedure between them, CNiL press release "Google privacy policy: six European data protection authorities to launch coordinated and simultaneous enforcement actions", 2 April 2013; available at http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo/; last visited on 25 April 2013.

Following up on the issue raised by the Google case, the Article 29 Working Party simultaneously published an opinion on purpose limitation[68], it which makes it clear that it views such aggregation of data types and purposes as incompatible with the existing legal framework. In addition, the opinion emphasises that vague or general purposes included in providers' privacy policies (for example, "improving user experience" or "marketing") will not usually meet the requirements of the purpose limitation principle set out in Article 6(1)(b) of the Data Protection Directive, that in turn affects the scope of the consent that users can give. Nevertheless, it is generally acknowledged that the consent concept as included in the Directive has not kept up with technological changes and is in acute need of reform.

Going forward, the initial version of Article 4(8) of the draft Regulation responds to that challenge by re-defining the data subject's consent as the

> *"freely given, specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement [to processing]".*

In contrast to the wording of the current Directive, the Regulation would therefore specifically require that all consent must be **explicit**.

While this definition is in line with recommendations that were made by the Article 29 Working Party in 2011, it markedly differs from the most recent interpretation of consent adopted by the ICO. For data controllers established in the UK, where they are given significant license to work on the basis of implied consent for many processing activities, the need for explicit consent would therefore require a major change in practice.

Although, for internet users, the new definition would undoubtedly have a positive effect (in that they would at the very least be required to make a clear statement of assent to the online provider's privacy policy or to take a clear affirmative action, such as ticking a box) it is at least doubtful whether this change in business practice would provide sufficient protection for their personal data in the long term.

By far the greater problem with regard to the use of consent in an online environment is the nature of online contracts themselves. Generally described as "adhesion contracts", the business terms and privacy policies of online providers are normally drafted in favour of those providers and are not negotiable. Their "take-it-or-leave-it" nature leaves the user with a choice either to adhere to the provider's conditions or not to use their service at all.

It is currently possible to identify four distinct possible 'fixes' for the problems arising from SNS providers' reliance on consent as a legal ground for data processing. These include market forces, technical features, co-regulatory or self-regulatory control and industry standards and user education.

Market forces

Some commentators claim that if left to their own devices, market forces will naturally arrive at an optimal level of privacy protection by offering consumers as much privacy as they actually value[69] and ask for. Those commentators argue that if government intervenes it may artificially distort markets in favour of some technologies and against others[70]. Rejecting this view, Edwards and Brown point out that consent given by many SNS users, especially young and inexperienced users, is almost always based on a misapprehension of risks[71].

---

[68] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP203), 2 April 2013; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; last visited on 25 April 2013.

[69] See, for example, P.H. Rubin & T.M. Lenerd Privacy and the commercial use of personal information (Boston: Kluwer Academic Publishers, 2001) (finding no failures in the market for personal information and recommending against government intervention).

[70] See, e.g., R. C. Picker, Competition and Privacy in Web 2.0 and the Cloud, U. Chi. L.& Econ. Working Paper 414, 2008 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985 (last visited 14 July 2010).

[71] L. Edwards and I. Brown, Data Control and Social Networking: Irreconcilable Ideas?' in A. Matwyshyn (ed), Harboring data: information security, law and the corporation (Stanford: Stanford University Press, 2009).

> *'It is in human nature to want jam today – fun and frivolity – over jam tomorrow – safety and security in some murky future where relationships, job opportunities and promotions may be pursued.* [72]

This is confirmed by sociological and criminological literature, which has indicated that, universally, consumer perceptions of future versus current risks are fundamentally flawed[73]. A lack of risk awareness in the main target group, however, may have a distorting effect on the market in question. Viewing the level of actual or potential public dissatisfaction with SNS' approach to privacy protection as the only factor determining a user's decision on which SNS provider to use ignores the fact that users will make that choice based on a variety of factors.

As a result, market forces are likely to be affected by factors other than simple user demand for the best privacy protection. For example, the network effect[74] created by popular services is likely to bind users closer to individual services (and may therefore indirectly limit their ability to exercise their "market power") until long after they have reached a level of dissatisfaction with the service that would normally prompt them to move to a competitor. Market forces on their own are therefore unlikely to solve the problems created by the use of consent in an SNS context.

Technical features

Some scholars advocate a 'code solution' that would allow users to control their personal information through, for example, the adjustment of privacy settings. Kesan and Shah argue that such settings would be an expression of the user's personal autonomy and would "provide users with agency" [75]. Users have a choice in the matter: they can go with the default option or choose another setting. However, Kesan and Shah also acknowledge that defaults shape norms and create culture by providing a recommendation to the user[76]. To this extent there is a danger that defaults can disempower users as they

> *"will be not be seen as defaults but as unchangeable. After all, if people don't know about defaults, they will assume that any alternative settings are impossible or unreasonable".*[77]

Edwards and Brown also emphasise the issue of user competence and user inertia. They argue that many users will not ever try to find out that settings other than the default exist, "whether through ignorance, fear or simple lack of time or energy or imagination"[78].

As has already been explained, there is now a growing tendency among SNS providers to use technical means, in the form of default privacy settings, to obtain user consent to a variety of data processing activities. In most cases, users are free to change defaults set to "public" but only by clicking their way through a variety of often complex and sophisticated choices. While this is ostensibly a way to grant users more control over the way in which they share their personal

---

[72] ibid., 221.

[73] See further D Apgar (2006) "Risk Intelligence", Harvard Business School Press; J Rauhofer (2008) "Privacy is dead, get over it! Information privacy and the dream of a risk-free society", Information & Communications Technology Law, Volume 17, Issue 3, 185-197.

[74] The term 'network effect' or 'network externality' commonly describes a situation where the the utility that a user derives from the consumption of a specific good or service increases with the number of other users consuming the same good or service, see M. L. Katz and C. Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) *The American Economic Review*, Vol. 75, No. 3, 424-440. This effect is particularly strong in relation to services that rely on the use of communications technologies; services, in other words, that require users' interaction with other users to fulfil their intended function. For example, the utility a user derives from buying a telephone depends directly on the number of other users connected to the telephone network.

[75] J. P. Kesan and R. C. Shah, Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics (2006) Notre Dame Law Review, Vol. 82, 583-634.

[76] ibid.

[77] ibid.

[78] L. Edwards and I. Brown at FN71. See also J. T. L. Grimmelmann, Facebook and the Social Dynamics of Privacy (2009) Iowa Law Review, Vol. 95, No. 4, 1137. Also at SSRN: http://ssrn.com/abstract=1262822 (last visited 14 July 2010). Grimmelmann argues that users will disable any feature that protects their privacy too much since, in social networking environments, anything that makes it harder for them to share information is a bug, not a feature. Edwards and Brown counter that restrictive privacy settings would at least make users aware, that there is such a thing a privacy defaults.

information, privacy groups as well as data protection regulators have identified a number of problems with this approach.

In particular, they point out that changing default settings can be a laborious undertaking and often little information is provided to users on how the default settings can be reversed and how users' objection to certain forms of processing or their withdrawal of consent can be signified. Again, market leader Facebook has had the dubious honour of producing the headlines in this respect. A graphic published by the New York Times in May 2010 shows that to manage their privacy on that site, at the time, users had to navigate through 50 settings with more than 170 choices[79].

It is interesting to note that the 'bewildering tangle of options' thus revealed was itself the result of a substantial overhaul by Facebook[80] of its privacy settings following a reprimand, in July 2009, by the Canadian Privacy Commissioner. The Commissioner had criticised Facebook for having "serious privacy gaps in the way the site operates"[81] and had recommended more transparency, to ensure that the site's users have the information they need to make meaningful decisions about how widely they share personal information. Although this shows that SNS providers are taking steps to make adjustments to their terms of use and default settings in order to avoid a regulatory backlash, it seems that those steps all too often fail to actually address the underlying problems. For example, like many SNS providers, Facebook has taken on board criticism that its privacy setings were too complex and has made it considerably easier for those seeking to protect their privacy to access and amend those settings. However, problems remain particularly in those cases where the user's privacy choices are overridden in the course of the introduction of new features[82] or if users make changes to their profile or the content they upload. Anectodal evidence suggests, for example, that uploading a new profile photo will automatically make that photo accessible to the open internet, even if the user had chosen to restrict access to the previous photo to "friends only".

The draft Regulation acknowledges the difficulties users face when trying to control the purposes for which SNS providers and their customers may process their personal data through the use of privacy settings. Article 23(1) requires the data controller, both when determining the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject ("privacy by design"). Similarly, Article 23(2) states that data controllers must "implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing" (privacy-by default"). In addition, those mechanisms must ensure that "data is not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage". While these are admirable sentiments, it is difficult to see, how these requirements can be enforced in view of the constantly changing technology used by online providers. Although Article 23(3) gives the European Commission the right to adopt delegated acts for the purpose of specifying further criteria and requirements for the "appropriate measures and mechanisms" to be taken, the considerations already discussed with regard to Article 6(5)[83] also apply here. As an executive body, the Commission lacks both the legitimacy and the necessary qualifications to adopt provisions of this kind so that the assessment of such measuers should be left to the EDPB and the national data protection authorities. By the same token, the Commission's right

---

[79] See FN64. In response to wide-spread criiticism, Facebook founder Mark Zuckerberg announced on 24 May 2010 that the site 'is to revise its privacy settings within weeks to make it simpler for people to keep their information private', see 'Facebook to tweak privacy settings, says Zuckerberg', Guardian, 24 May 2010 at http://www.guardian.co.uk/technology/2010/may/24/facebook-revise-privacy-zuckerberg (last visited 30 October 2012).

[80] Facebook Press release, 27 August 2009 at http://www.facebook.com/press/releases.php?p=118816 (last visited 4 March 2010).

[81] Report of Findings by the Office of the Privacy Commissioner of the Canada into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act, 16 July 2009 at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm (last visited 4 March 2010).

[82] See, for example, G Cluely, "Facebook changes privacy settings for millions of users - facial recognition is enabled", 7 June 2011; available at http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/; E Brown "Facebook Timeline privacy concerns deepen as rollout begins", 19 December 2011; available at http://www.zdnet.com/blog/feeds/facebook-timeline-privacy-concerns-deepen-as-rollout-begins/4424; and last visited on 25 April 2013;.

[83] See "Legitimate interest" above.

to "lay down technical standards for the requirements"[84] is unlikely to provide sufficient protection of internet users' privacy rights given the rapid pace of technological development.

Co-regulatory or self-regulatory control and industry standards

Because it is unlikely that users would challenge contractual terms until after harm has been caused to them by the misuse of personal data, efforts have been made to protect user privacy *ex ante* through model contracts for SN services, non-binding regulatory guidance[85] or industry or co-regulatory codes of conduct. In the US, Facebook is unusual among the major SNS providers in being signatory to TrustE, the industry privacy seal program. This means, in principle, that Facebook's privacy policy is subject to third party review. In the EU, SNS providers such as Bebo, Facebook, Google and Microsoft signed an agreement on "Safer Social Networking Principles for the EU" in February 2009[86], which includes seven guiding principles for providers, covering issues such as raising awareness through education and training, and empowering users through technology and tools. However, in a report made available by the European Commission in September 2011, it found that while some steps had been taken, problems still existed with regard to tools available on the sites. It also found that only two of the signatories of the agreement had default settings which make minors' personal profiles accessible only to their approved list of contacts[87]. One could therefore argue that some SNS providers use the co- and self-regulatory approach to stave off more drastic regulatory measures. However, without at least the threat of such measures, it is doubtful whether the motivation of online services will be sufficient to ensure the protection of their users' privacy where this seriously affects their revenue streams and with it their prospects of commercial success.

Educational measures

Until now, regulators seem to have put most of their effort into advising users how to act wisely on SNS. In the UK, the Information Commissioner has launched a website aimed at helping young people understand their information rights[88]. A similar website was launched in Germany supported by the state data protection commissioner in Saarland[89] Although initiatives like these are important, there is currently very little evidence that they are in fact successful in overcoming user apathy. Further research is therefore required into the effectiveness of educational measures, given other social and cultural factors that may play a role in users' choice of provider. Nevertheless, given the role that online services play in the development, social life and learning experience of most children at least in the developed world, greater emphasis should be placed on promoting an increased awareness of information rights and obligations in early-years and secondary education for children[90].

Additional rights and safeguards included in the draft Regulation

In addition to the provisions described above, which largely constitute revisions of existing requirements included in the Data Protection Directive, the draft Regulation also includes a number of additional rights and safeguards, designed to protect data subjects' interests particularly in the online environment. While a detailed analysis of these additional rights goes beyond the scope of this article,

---

[84] Article 23(4), draft Data Protection Regulation.

[85] See, for example, the 'Good practice guidance for the providers of social networking and other user interactive services', UK Home Office, 4 April 2008.

[86] European Commission press release "Digital Agenda: social networks can do much more to protect minors' privacy - Commission report", 30 September 2011; available at http://www.saferinternet.eu/c/document_library/get_file?uuid=9ea87190-cfe8-476a-babb-59935aa08892&groupId=12160; last visited on 25 April 2013.

[87] 'Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report', European Commission, January 2010 at http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf (last visited on 26 May 2010).

[88] At http://www.ico.gov.uk/youth.aspx (last visited 1 November 2012).

[89] At http://www.datenparty.de/ (last visited 1 November 2012).

[90] C Ewart and K Tisdall (2012) "Embedding information rights in the primary and secondary education systems of the United Kingdom: Phase 2 report for the Information Commissioner's Office", 31 March 2012; vailable at http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/embedding_information_rights_phase_2_report.ashx; last visited on 25 April 2013.

reference can be made to (1) an extended right of the data subject to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data (right to be forgotten and to erasure)[91]; (2) a new right to data portability, which would enable the data subject to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject[92]; and (3) a right not to be subject to measures based on profiling[93]. The latter includes measures that produce a legal effect concerning or significantly affecting the data subject, which is based solely on automated processing intended to evaluate certain personal aspects relating to him or to analyse or predict his performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

Taken together, these rights may well have an impact on the level of control internet users can exercise in the context of their relationships with SNS providers. The right to data portability, which is designed to help Internet users to overcome network effects inherent in the services of the first-to-market incumbents, might serve to address some of the power imbalance referred to above. However, the way in which it enables, if not encourages, the wider distribution of personal data sets to more than one provider must be kept under observation before the provision's final impact can be assessed.

Both the right to be forgotten and erasure and the right to be free from measures based on monitoring face multiple criticism[94] regarding both their technical feasibility and their suitability to protect Internet users' true interest with the UK actually seeking an opt-out from the former[95]. Given that negotiations about the content of the draft Regulation are ongoing, it remains to be seen which of these provision will make it into the final draft unchanged.

Conclusion

Despite the fact that both national and EU regulators and the EU legislator are clearly aware of the need to improve the protection of internet users' privacy and data protection rights, current thinking in this area seems to have stepped away from many of the conceptual foundations that informed data protection laws when they were first adopted in the 1970s and 80s. In particular, there now seems to be an increased call for a more "risk-based" approach to data protection that argues that where little or no harm is likely to be incurred by the data subject through individual processing activities, the interests of data controllers in the free flow of data should be given preference when exploiting personal data for their own commercial or administrative needs and that the regulatory burden should be kept low[96]. In this context, the definition of "harm" is all to often reduced to mere economical loss and is looked at entirely from the perspective of the here and now with little attention being paid to the potential unintended consequences that extensive data processing activities may be found to have in the future. This approach, which is germane to both the property-rights based approach and the fair processing paradigm, is a long way away from the assessment by the German Constitutional Court in its 1984 *Census* decision that "under the conditions of automated data processing, there no longer is such a thing as 'irrelevant' data"[97].

---

[91] Article 17, draft Data Protection Regulation.

[92] Article 18, draft Data Protection Regulation.

[93] Article 18, draft Data Protection Regulation.

[94] See, for example, Spiegel online "'The Right to Be Forgotten': US Lobbyists Face Off with EU on Data Privacy Proposal", 17 October 2012; available at http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html; T Brewster "Facebook: EU's 'Right To Be Forgotten' Will Enforce More User Tracking", TechWeek Europe, 6 December 2012; available at http://www.techweekeurope.co.uk/news/facebook-europe-right-to-be-forgotten-tracking-101253; last visited on 25 April 2013.

[95] O Bowcott "Britain seeks opt-out of new European social media privacy laws", Guardian online, 4 April 2013; available at http://www.guardian.co.uk/technology/2013/apr/04/britain-opt-out-right-to-be-forgotten-law; last visited on 25 April 2013.

[96] This position was most recently reaffirmed by the ICO in its submission to the House of Commons Justice Committee that was tasked with assessing the impact of the EU reforms. The ICO argued in favour of its own "better regulatory approach of risk-based proportionate intervention", paragraph 50; see "Report of the HoC Justice Committee on the European Union Data Protection framework proposals", 24 October 2012, available at http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/57202.htm, last visited 1 November 2012.

[97] FN8, paragraph 158.

In reality, the threat that the on-going technological innovation presents to EU citizens' fundamental right to privacy is only increasing. The term "Big Data" has turned into a watchword for the increasing power that the unrestricted collection and use of individuals' personal information has bestowed on both public and commercial players. Unless steps are taken now to ensure that the information privacy rights we have taken for granted in an offline environment are also protected online, the opportunity to entrench those rights in the digital space may be missed for a very long time, if not forever.

With every new data-hungry application and business model that is developed, a new infrastructure embeds itself into our daily lives. This may have long-term consequences that we are not yet able to foresee but which may change the delicate balance of power between individuals, commercial entities and public bodies that our democratic constitutions were designed to create and maintain. This may ultimately not only affect the rights and freedoms of Internet users, but also the competitiveness of online businesses and the foundations of democratic government itself.

It is already possible to observe an increasing lack of trust on the part of Internet users in certain online services. Despite the initial attraction of those services, fuelled by curiosity and a natural human desire to communicate with others, and the network effect, which continues to bind users to those services once they have joined, we may yet reach a tipping point when that lack of trust begins to outweigh both those factors. A lack of effective privacy protection could thus ultimately have a negative impact on individuals' willingness to use online services to their full potential both in the private arena and for the purpose of political participation.

Many EU member states already recognise this problems and are taking unilateral steps to address the most pressing issues at national level[98]. To ensure the protection of both its citizens' rights and its businesses' competitiveness as well as to avoid the multi-speed development of a new regulatory framework for online services, the EU institutions must now also follow up their manifold statements of intent with considered and well-balanced legislation. It is at least doubtful whether the current proposals for a reform of the EU data protection framework are capable of achieving this aim even if they were adopted in their current form. Any further watering down of the level of protection that this version provides might seriously put at risk more than just an individual or property right.

In particular, there is a strong case to be made for the contention that EU data protection law should "go back to its roots" and revisit the principle of data minimisation. This principle provides by far the strongest safeguard against the abuse of personal data both for commercial and for political purposes as data that has never been collected is not available for covert or overt, lawful or illegitimate re-purposing. An *ex ante* data minimisation principle is therefore likely to be more effective in protecting individuals' information privacy rights than *ex post facto* controls of processing activities in relation to data that is already in existence.

In this context, some recognition must be given to the way in which the draft Regulation already seeks to strengthen this principle. Where the current Data Protection Directive merely stipulates that personal data should only be collected for "specified, explicit and legitimate purposes"[99], Article 5(c) of the draft Regulation would limit the data controller's right to process personal data "to the minimum necessary in relation to the purposes for which they are processed". This mirrors to some extent

---

[98] See, for example, measures taken by the independent data protection Commissioner for German state Schleswig-Holstein against the tracking of Facebook users and non-users through the "Like" button, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, "ULD to website owners: „Deactivate Facebook web analytics", 19 August 2011, available at https://www.datenschutzzentrum.de/presse/20110819-facebook-en.htm; and the effect of the Irish data protection authorities recommendations for measures that need to be taken by the same company to ensure compliance with Irish data protection laws, Irish Data Protection Commissioner, "Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU", 21 September 2012, available at https://www.dataprotection.ie/viewdoc.asp?Docid=1233&Catid=66&StartDate=1+January+2012&m=n, both last visited on 31 October 2012.

[99] Article 6(1)(b), Data Protection Directive and Article 5(a), draft Data Protection Regulation.

the requirement included in §3a of the German Data Protection Act[100] which states that the collection, processing and use of personal data must be guided by the objective to process as little data as possible. The problem with regard to data minimisation is, of course, that its success is strongly dependent on the enforcement capabilities of data protection authorities. Without strong powers of inspection and oversight, even the best data minimisation principle is likely to develop into "a custom more honoured in the breach than the observance".

Similarly, clear similarities can be identified between the relationship between users and providers of online services (specifically SNS) and consumers and businesses. In both cases, the parties clearly possess unequal bargaining power when entering into a contractual relationship. Outside a clear regulatory framework, this can lead to the user/consumer being forced to transact on the basis of contractual provisions that were designed to benefit the business/provider. In the context of a consumer sale, this could mean that the consumer would have to accept, for example, far reaching limitations of liability, restrictions on the consumer's ability to terminate the contract in case of non-performance or reversals of the burden of proof in those cases. Consumer protection laws in almost all jurisdictions therefore provide a framework that, while restricting the consumer's personal autonomy to a certain extent, also protects him from the most unreasonable demands of those in a stronger bargaining position. In this context, the restriction of the user's contractual freedom is accepted in the interest of enforcing a fairer balance between the perceived commercial interests of both parties. In many cases, this is achieved by the adoption of certain "good faith" requirements on the part of both parties combined with an agreed list of "behaviours" or contractual clauses that would make the contractual relationship between the parties void or voidable.

Given that personal data has now replaced money as a form of payment for many of the services rendered in an online context, there may therefore be a case for a legal framework that protects users' personal information along similar lines. As outlined above, in the context of data protection law, this approach could entail imposing restrictions on the type of processing activities to which a data subject can lawfully consent as well as restrictions on the type of processing activities a data controller can justify through reliance on the "legitimate interest condition". As is already the case in consumer protection law, any processing carried out in violation of such stipulations would be unlawful and render the controller in breach of his data protection obligations.

While it cannot be denied that an effective protection of information privacy in an online context may ultimate require the use of a variety of regulator constraints, including a change in the social norms that govern the disclosure, sharing and use of personal information; the use of code-based solutions like privacy-by-default and privacy-by-design technologies that restrict the collection of personal data *ab initio*; and a developing market in privacy-friendly applications, services and business models, it seems obvious that all of these approaches would not only be complemented, but also facilitated, by a stronger legal framework. To achieve its full potential, such a framework must perceive information privacy as a means to protect individuals' rights both as consumers (individual right to privacy) and as citizens of democratic systems with a responsibility to contribute to the upholding of those systems' moral and political values (privacy as a common good). To sacrifice one or the other in the name of economical growth or political convenience is to open the door to potential abuse by a variety of public and private entities with long-term consequences that we may not yet be able to conceive.

[100] Bundesdatenschutzgesetz (BDSG).